USE OF ISOGENIES FOR DESIGN OF CRYPTOSYSTEMS

Techniques are disclosed to provide public-key encryption systems. More particularly, isogenies of Abelian varieties (e.g., elliptic curves in one-dimensional cases) are utilized to provide public-key encryption systems. For example, the isogenies permit the use of multiple curves instead of a single curve to provide more secure encryption. The techniques may be applied to digital signatures and/or identity based encryption (IBE) solutions. Furthermore, the isogenies may be used in other applications such as blind signatures, hierarchical systems, and the like. Additionally, solutions are disclosed for generating the isogenies.